In the Claims

1-22 (canceled)

23. (previously presented) The method of claim 26, further comprising said host device routing said data to said firewall device to be processed by said hardware implemented firewall, said routing taking place at a physical layer in said data stack.

24. (previously presented) The method of claim 26, further comprising:

f) sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified.

25. (canceled)

26. (currently amended) A method of providing security in a network having a network interface device that makes a network connection without a firewall capability in said communication interface device that is required by the network for data transfer between the network and a host device using the network interface device, said method comprising:

a) allowing a connection to said network to be established when said host device uses said network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to said host device;

b) receiving data from said network over said connection establish via said communication interface device;

c) processing said data with said hardware implemented firewall; ~~and~~

d) transferring said processed data to said host device~~, wherein said data is processed by said hardware implemented firewall~~; and

e) performing a configuration integrity check of a software component on a host device, wherein said configuration integrity check is performed before said network connection is allowed, wherein said connection is allowed only if said configuration integrity check ~~passes;~~ passes.

27. (previously presented) The method of claim 26, wherein e) comprises performing said configuration integrity check by performing a hash on said software component to produce a hash value and comparing said hash value with a stored hash value.

28. (original) The method of claim 27, wherein said stored hash value resides on said firewall device.

29. (original) The method of claim 27, further comprising:

f) sending an alert if said configuration integrity check fails.

30. (original) The method of claim 29, further comprising:

g) storing an alert if said configuration integrity check fails.

31. (previously presented) The method of claim 26, further comprising:

f) swapping resource spaces in said host device that are reserved for said communication interface device and said firewall device, wherein said host device treats said communication interface device as said firewall device and vice versa; and

g) said communication interface device transferring data received from said network in b) to said firewall device, wherein said firewall device processes said data with said hardware implemented firewall.

32. (previously presented) The method of claim 26,further comprising:

f) transferring data to be transferred over said network by said communication interface device to said firewall device; and

g) processing said data with said hardware implemented firewall, wherein said data is processed by said hardware implemented firewall before it is transferred over said network connection established via said communication interface device.

33. (previously presented) The method of claim 32, wherein said f) comprises said host device routing said data to said firewall device before it is sent to said communication interface device, said routing taking place at a physical layer in said data stack.

34. (previously presented) The method of claim 26, further comprising:

f) performing a configuration integrity check of a software component on said host device; and

g) sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified.

35. (original) The method of claim 34, further comprising:

g) sending an alert if said configuration integrity check fails.

36-39 (canceled)

40. (currently amended) A method of providing security in a network having a network interface device that makes a network connection without a firewall capability in said communication interface device that is required by the network for data transfer between the network and a host device using the network interface device, said method comprising:

allowing a connection to said network to be established when said host device uses said network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to said host device;

receiving data from said network over said connection establish via said communication interface device;

processing said data with said hardware implemented firewall;

transferring said processed data to said host device, ~~wherein said data is processed by said hardware implemented firewall~~; and

performing a configuration integrity check of a software component on said host device by performing a hash on said software component to produce a hash value and comparing said hash value with a stored hash value.

41. (previously presented) The method of claim 40, further comprising said host device routing said data to said firewall device to be processed by said hardware implemented firewall, said routing taking place at a physical layer in said data stack.

42. (previously presented) The method of claim 40, further comprising:

sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified.

43. (previously presented) The method of claim 40, wherein said configuration integrity check is performed before said network connection is allowed and wherein said connection is allowed only if said configuration integrity check passes.

44. (previously presented) The method of claim 40, wherein said stored hash value resides on said firewall device.

45. (previously presented) The method of claim 40, further comprising:

sending an alert if said configuration integrity check fails.

46. (previously presented) The method of claim 45, further comprising:

storing an alert if said configuration integrity check fails

47. (previously presented) The method of claim 40, further comprising:

swapping resource spaces in said host device that are reserved for said communication interface device and said firewall device, wherein said host device treats said communication interface device as said firewall device and vice versa; and

said communication interface device transferring data received from said network to said firewall device, wherein said firewall device processes said data with said hardware implemented firewall.

48. (previously presented) The method of claim 40, further comprising:

transferring data to be transferred over said network by said communication interface device to said firewall device; and

g) processing said data with said hardware implemented firewall, wherein said data is processed by said hardware implemented firewall before it is transferred over said network connection established via said communication interface device.

49. (previously presented) The method of claim 48, wherein said transferring data to be transferred over said network by said communication interface device to said firewall device comprises:

routing said data from said host device to said firewall device before it is sent to said communication interface device, said routing taking place at a physical layer in said data stack.

50. (previously presented) The method of claim 48, further comprising:

performing a configuration integrity check of a software component on said host device; and

sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified.

51. (previously presented) The method of claim 50, further comprising:

sending an alert if said configuration integrity check fails

52.-63. (cancelled)